AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) An automation security system, comprising:

an automation asset operatively coupled to a network communication channel, an automation asset comprises at least an automation control device and implements the following:

an extensible factory protocol to transport data between the automation asset and [[an]] a remote automation asset on a remote network communication channel, the extensible factory protocol is a control-specific transport mechanism for data exchange between automation assets that ~~encodes~~ is adapted to include at least one security field within the extensible factory protocol to exchange data with the remote automation asset, the security field of the extensible factory protocol authenticates at least one of a requestor of the data or a supplier of the data.

2. (Previously Presented) The system of claim 1, the security field further comprises path information to identify a requester or supplier of a connection.

3. (Original) The system of claim 2, the path information facilitates non-connected data access by sending out an open-ended message.

4. (Currently Amended) The system of claim 1 the automation asset further comprises at least one of a controller, a communications module, a computer, a sensor actuator, a network sensor, an I/O device, Human Machine Interface (HMI), an I/O module, or a network device.

5. (Previously Presented) The system of claim 1, the network communications channel is established across at least one of: a control network, factory network, information network, private network, instrumentation network, a wireless network, or a public network.

6-8. (Cancelled)

9. (Previously Presented) The system of claim 1, the extensible factory protocol includes at least one of: a time component to mitigate replay attacks, a message integrity component, a digital signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, or a dynamic security adjustment field.

10. (Currently Amended) The system of claim 1, the extensible factory protocol ~~is adapted to at least one of:~~ comprises a Control and Information Protocol (CIP) ~~or an object model that protects configuration of and transport of data between intelligent devices~~ having a path segment that has been adapted to include a segment identifying a requestor of a connection between automation assets and employed to authenticate the requestor.

11. (Currently Amended) The system of claim 1, ~~further comprising a component to~~ the control-specific transport mechanism is further adapted to at least one of: provide source validation for identification, perform message digest checking for integrity checking, perform check sum tests, provide integrity mechanisms, provide encryption mechanisms, or provide refresh security protocols.

12. (Previously Presented) The system of claim 1, the extensible factory protocol facilitates at least one of an identification, an authentication, an authorization, or a ciphersuite negotiation to establish network trusts.

13. (Previously Presented) The system of claim 1, the extensible factory protocol is associated with a protocol supporting at least one of: a Temporal Key Interchange Protocol (TKIP) or a wireless protocol.

14. (Previously Presented) The system of claim 1, the extensible factory protocol employing at least one of: an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller-Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPeCT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol, or a Cellular Digital Packet Data (CDPD) protocol.

15. (Previously Presented) The system of claim 1, the network communications channel employing at least one of: a Control and Information Protocol (CIP) network, a DeviceNet network, a ControlNet network , an Ethernet network , DH/DH+ network , a Remote I/O network, a Fieldbus network, or a Profibus network.

16. (Original) The system of claim 1, further comprising a security field to limit access based upon line of sight parameters.

17. (Currently Amended) A method [[to]] that facilitates factory automation network security, comprising:

determining real-time data transfer requirements for automation devices in an industrial automation system;

determining network security requirements for communication between the automation devices ~~of an industrial automation system including a requirement for real-time performance~~;

adapting a wireless security protocol for communication between the automation devices ~~of the industrial automation system by lowering the security requirements if real-time performance is required~~ based on the real-time data transfer requirements and the network security requirements;

employing the wireless security protocol in communication between the automation devices of the industrial automation system; ~~and~~

dynamically selecting a ~~lightweight or heavyweight~~ first encryption mechanism ~~based the network security requirements~~ for the wireless security protocol during data transfers having a performance requirement exceeding a predetermined level, and selecting a second encryption mechanism for the wireless security protocol during data transfers having a performance requirement below the predetermined level[[.]], the second encryption mechanism providing a higher degree of encryption than the first encryption mechanism; and

providing a security time-out within the wireless security protocol that times-out data transactions between the automation devices after a predetermined time duration until a subsequent determination of real-time data transfer requirements and network security requirements is performed.

18. (Currently Amended) The method of claim 17, further comprising incorporating a Temporary Key Interchange Protocol (TKIP) protocol within an automation protocol.

19. (Previously Presented) The method of claim 17, further comprising utilizing at least one of: a Temporal Key Interchange Protocol (TKIP) or an Elliptical function in the wireless security protocol.

20. (Currently Amended) A method to facilitate automation network security, comprising:

determining a need for real-time communication with an automation control device;

establishing a communications session with a remote automation control device across an automation control network ~~*via* a heavyweight encryption mechanism in~~ using a security protocol ~~employed in the communication session~~ having a first encryption mechanism if it is determined that real-time communications is not needed; ~~and~~

exchanging data between the automation control device and the remote automation control device ~~in accordance with real-time communications~~ *via* a ~~lightweight~~ second encryption mechanism in the security protocol ~~that induces minimal impact on system performance~~ if real-time communication is needed[[.]], wherein the first encryption mechanism provides a higher degree of encryption that the second encryption mechanism; and

providing a security time-out within the security protocol that times-out the communications session after a predetermined amount of time until a subsequent determination for real-time communication is made.

21. (Currently Amended) The method of claim 20, further comprising dynamically switching between the ~~heavyweight~~ first encryption mechanism and the ~~lightweight~~ second encryption mechanism during the real-time communications in accordance with real-time communication needs.

22. (Currently Amended) The method of claim 20, ~~the lightweight encryption mechanism includes~~ wherein exchanging data between the automation control device and the remote automation device *via* the second encryption mechanism comprises providing an encryption mechanism that includes at least one of: time component to mitigate replay attacks, a message integrity component, a digital signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, or a dynamic security adjustment field.

23. (Cancelled)

24. (Currently Amended) An automation security system, comprising:

means for encoding a security component within a factory protocol, the factory protocol is ~~specifically~~ adapted for data exchange between automation assets in a control domain and includes at least one of a security parameter or a performance parameter that is determined by at least one automation asset;

means for transmitting the security component and the factory protocol across a network between an automation asset in the control domain and an automation asset remote to the domain using a first standard of security if the at least one of a security parameter or a performance parameter dictates that real-time performance is required, and a second standard of security if the at least one of a security parameter or a performance parameter dictates that real-time performance is not required, the first standard of security is lower than the second; ~~and~~

means for the at least one automation asset to decode the security component in order to facilitate a secure communications channel across the network[[.]]; and

means for enforcing a time limit on data exchange between the automation asset in the control domain and the automation asset remote to the domain, after which time limit the data exchange is timed-out until the performance parameter is re-determined.

25. (Currently Amended) An automation security system, comprising:

a control device that utilizes an extensible factory protocol, the extensible factory protocol is implemented for data exchange between control devices across more than one communication network and is adapted to include intrusion detection capability;

a parameter detection component that detects at least one of a security or a performance parameter that extends the factory protocol, the factory protocol utilizes a ~~lightweight~~ first encryption mechanism if the at least one of a security or performance parameter dictates that real-time performance is required[[,]] and a ~~heavyweight~~ second encryption mechanism if the at least one of a security or performance parameter dictates that real-time performance is not required, wherein the second encryption mechanism provides a higher degree of encryption than the first encryption mechanism; ~~and~~

a time component encoded in the factory protocol that defines an amount of time after which data exchange between control devices is timed-out until the at least one of a security or performance parameter is re-evaluated; and

an intrusion detection component adapted for the extensible factory protocol to detect network attacks directed to the control device.

26. (Currently Amended) The system of claim 25, the intrusion detection component is at least one of a host-based component ~~and~~ or a network-based component.

27. (Previously Presented) The system of claim 25, the intrusion detection component is adapted to at least one of: an attack signature, an address, an address range, a counter, a location, a time, an event, a control list, a virus, or a Trojan executable.

28. (Currently Amended) A security violation detection methodology, comprising:

adapting an industrial network protocol in accordance with an intrusion detection technology; ~~and~~

monitoring the industrial network protocol for an attack *via* the intrusion detection technology, the monitoring is conducted at a first security level if real-time performance is requested between automation devices employing the industrial network protocol ~~in remote networks~~, and a second security level if real-time performance is not requested, the first security level is lower than the second;

automatically performing a security action after detecting the attack, the security action includes at least one of enabling an alarm, denying network access or removing a virus[[.]]; and

providing a time-based component within the industrial network protocol that defines an amount of time after which the real-time performance must be re-evaluated before data transactions between the automation devices are allowed to continue.

29. (Original) The method of claim 28, further comprising monitoring a network for flooding attacks.

30-31. (Cancelled)

32. (Previously Presented) The automation security system of claim 1, the extensible factory protocol maintains backward compatibility with an automation asset incapable of implementing the security field.